Notice of Allowability	Application No.	Applicant(s)	
	10/026,848	WANG, YNJIUN P.	
	Examiner	Art Unit	
	Mary Cheung	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☐ This communication is responsive to *RCE file 11/23/2005*.

2. ☒ The allowed claim(s) is/are *5,6,8 and 10-17*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with James Sheridan on February 3, 2006.

The application has been amended as follows:

Claims 1-4 have been canceled.

Claim 5 has been replaced to read

--5. A method of exchanging secured messages between first and second registered PEAD users over the internet and a server utilizing at least one PEAD, comprising the steps of:

a PEAD sender obtaining a PEAD receiver's public key using the receiver's user ID as an index from the server;

the sender creating a shared secret using the receiver's public key and said sender's own private key;

the sender then electronically encrypting a message with the shared secret, and sending the encrypted message appended with the sender's user ID and the receiver's user ID to the receiver;

the receiver receiving the encrypted message appended the sender's user ID and the receiver's user ID from the sender;

the receiver requesting only the sender's public key from the sender;

the receiver receiving the sender's public key from the sender;

the receiver decrypting the encrypted message by deriving the shared secret using the sender's public key and said receiver's own private key, wherein the encrypted message remaining encrypted while handled by the server.--

In claim 6 line 2, the word --user-- has been inserted before the word "ID";

Claim 7 has been canceled.

In claim 8 line 3, the word --user-- has been inserted before the word "ID";

Claim 9 has been canceled.

In claim 12 line 4, the word --user-- has been inserted before the word "ID";

In claim 14 line 3, the word "senders" has been changed to read --sender's--;

In claim 16 line 2, the word "senders" has been changed to read --sender's user-;

Allowable Subject Matter

3. Claims 5-6, 8 and 10-17 are currently pending as by the examiner's amendment. All the pending claims are allowed.

4. The following is an examiner's statement of reasons for allowance:

The closest prior art of Dorenbos (U. S. Patent 5,751,813) teaches an encryption server receives a first encrypted message and decrypts the encrypted message using a first key, yielding a decrypted message comprising a second encrypted message, an identification of a first recipient. The second encrypted message, the identification of the sender, and the identification of the first recipient are determined from the decrypted

message. The second encrypted message and the identification of the sender are encrypted with a second key, yielding a third encrypted message. The third encrypted message is transmitted to the first recipient.

In regarding to independent claim 5, Dorenbos taken either individually or in combination with other prior art of record fails to teach or suggest a sender creates a shared secret using a receiver's public key and said sender's own private key, the sender then encrypts a message with the shared secret and sends the encrypted message appended with the sender's user ID and the receiver's user ID to the receiver, the receiver decrypts the encrypted message by deriving the shared secret using the sender's public key and said receiver's own private key, wherein the encrypted message remaining encrypted while handled by the server.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Griffith et al. (U. S. Patent 4,825,050) discloses security transaction system.

Serbetciouglu et al. (U. S. Patent 5,719,918) discloses short message transaction handling system.

Harris (U. S. Patent 6,144,949) discloses radio frequency communication system with subscribers arranged to authenticate a received message.

Numao (U. S. Patent 6,377,688) discloses cryptographic communication system.

Hayosh (U. S. Patent 6,600,823) discloses enhancing check security system.

Article titled "Pretty Good Privacy" by Noor (UNIX Review v13n2, pp 31-38, February 1995, ISSN: 0742-3136).

Inquire

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mary Cheung whose telephone number is (571)-272-6705. The examiner can normally be reached on Monday – Thursday from 10:00 AM to 7:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell, can be reached on (571) 272-6712.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

The fax phone number for the organization where this application or proceedings is assigned are as follows:

(571) 273-8300 (Official Communications; including After Final Communications labeled "BOX AF")

(571) 273-6705 (Draft Communications)

Mary Cheung
Primary Examiner
Art Unit 3621
February 3, 2006

MARY D. CHEUNG
PRIMARY EXAMINER